Тема 3 Кіберзагрози у фінансовій системі Європи та України

Метою лекції є огляд поточних кіберзагроз, які існують у фінансовій системі Європи та України, їхньому впливу на фінансові установи та огляд заходів, що можна вжити для пом'якшення цих кіберзагроз

План

1. Змістовна сутність поняття «кіберзагроза» у фінансових системах
2. Сучасні типи кіберзагроз фінансової системи України та Європи
3. Аналіз факторів цифрової довіри

1. Змістовна сутність поняття «кіберзагроза» у фінансових системах

Кіберзагрози у фінансах – це загрози для фінансових систем і індустрії фінансових послуг, включаючи, але не обмежуючись, послуги інтернет-банкінгу, необанкінгу та грошові перекази, роздрібні платіжні системи, мобільні банківські та платіжні системи, цифрові валюти та інші фінансові послуги. Ці загрози можуть включати крадіжку інформації та коштів клієнтів, відмивання грошей, несанкціоновані перекази та інші зловмисні дії. Крім того, кіберзагрози можуть включати атаки на відмову в обслуговуванні, шкідливі програми та програми-вимагачі, фішинг, соціальну інженерію та витоки даних. Атаки на фінансові установи можуть мати серйозні ризики для безпеки клієнтів, операцій і фінансів.

Інноваційна трансформація політичної, економічної, соціальної сфери посилює залежність фінансової системи від цифрових рішень, стимулюючи необхідність посилення безпеки. У світлі ризику та потенційних наслідків кіберподій, фінансового шахрайства, посилення фінансової безпеки та стійкості кіберпростору є важливою місією внутрішньої безпеки для кожної країни. Так посилення заходів кібербезпеки для фінансових соціально-економічних об'єктів країн, які є членами Євросоюзу детально прописується в межах стратегічного плану Генерального директорату з інформатики 2020 – 2024 (DIGIT), який відіграє координаційну роль у розвитку інформаційних технологій та систем інформаційно-комінікаційних технологій [1]. Основною метою є формування безпечного та сучасного цифрового середовища, здатного забезпечити надійну, економічно вигідну та безпечну інфраструктуру та послуги, в ногу з новими методами роботи та спільної роботи, що узгоджуються із очікуваннями персоналу, громадян, бізнесу та зацікавлених сторін.

За результатами аналізу публікацій, що індексуються базою даних скопус за запитом «кіберзагрози у фінансах» із використанням програмного забезпечення VOSviewer дозволив сформувати 4 групи, в яких автори спільно використовують щонайменше 5-ти ключових слів із загальної кількості 1070 слів (табл. 1, рис. 1). Загальна кількість взаємозв'язв'ків між цими публікаціями складає 288 одиниць.

Таблиця 1. Топ 32 ключових слів

Кластер	Ключові слова
Кластер 1	штучний інтелект, блокчейн, кіберзагроза, кібербезпека, електронна комерція, фінанси, фінансові інституції, фінансовий сектор, фінтех, машинне навчання
Кластер 2	хмарні обчислення, критична інформаційна інфраструктура, криптографія, прийняття рішень, виявлення вторгнень, мобільна безпека, безпека, безпека систем, загроза безпеці
Кластер 3	комп'ютерна злочинність, злочинність, кібератаки, інформаційно-комунікаційні технології, шкідливе програмне забезпечення, безпека комп'ютерних мереж, персональні обчислення
Кластер 4	кібербезпека, інформаційний менеджмент, інформаційна безпека, оціюнювання ризику, управління ризиком, безпека даних

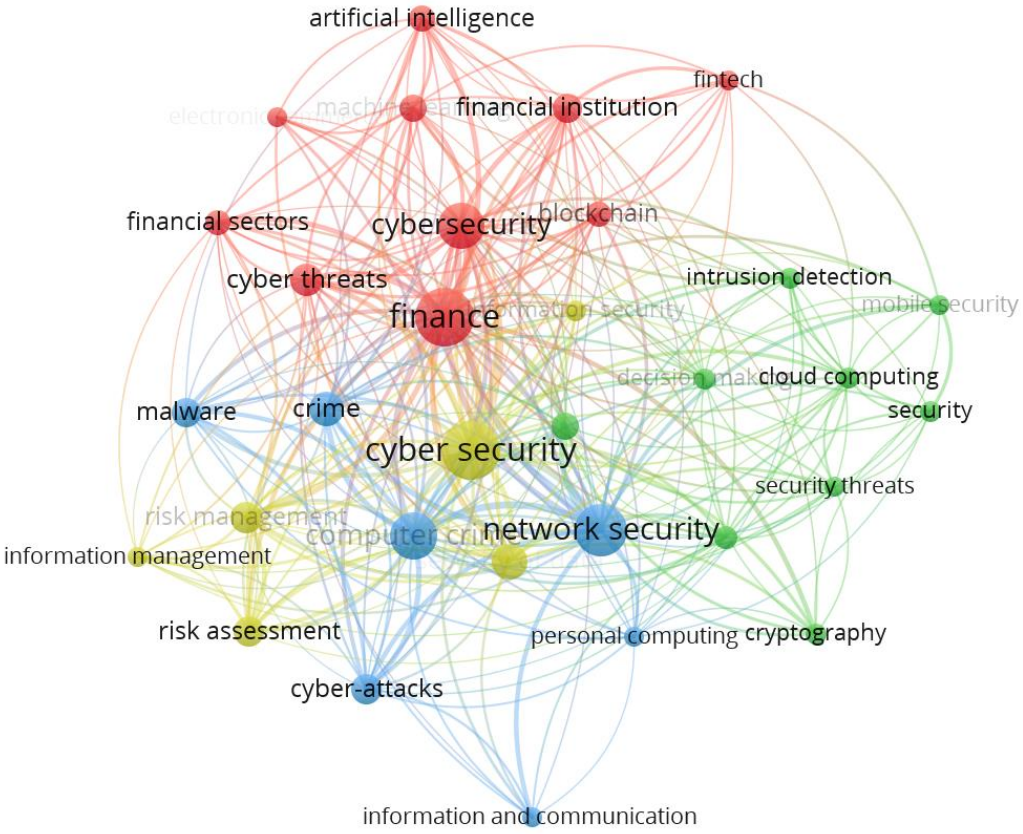


Рисунок 1. Хмара ключових слів за тематикою «кіберзагрози у фінансах»

В Положенні про організацію кіберзахисту в банківській системі України, поняття «критична інформаційна інфраструктура» визначається, як сукупність об'єктів критичної інформаційної інфраструктури банку, визначена об'єктом критичної інфраструктури в банківській системі України [2].

Динаміка публікацій в розрізі дослідження кіберзагроз у фінансових системах світу за знайденими ключовими словами відобрежана на рисунку 2.

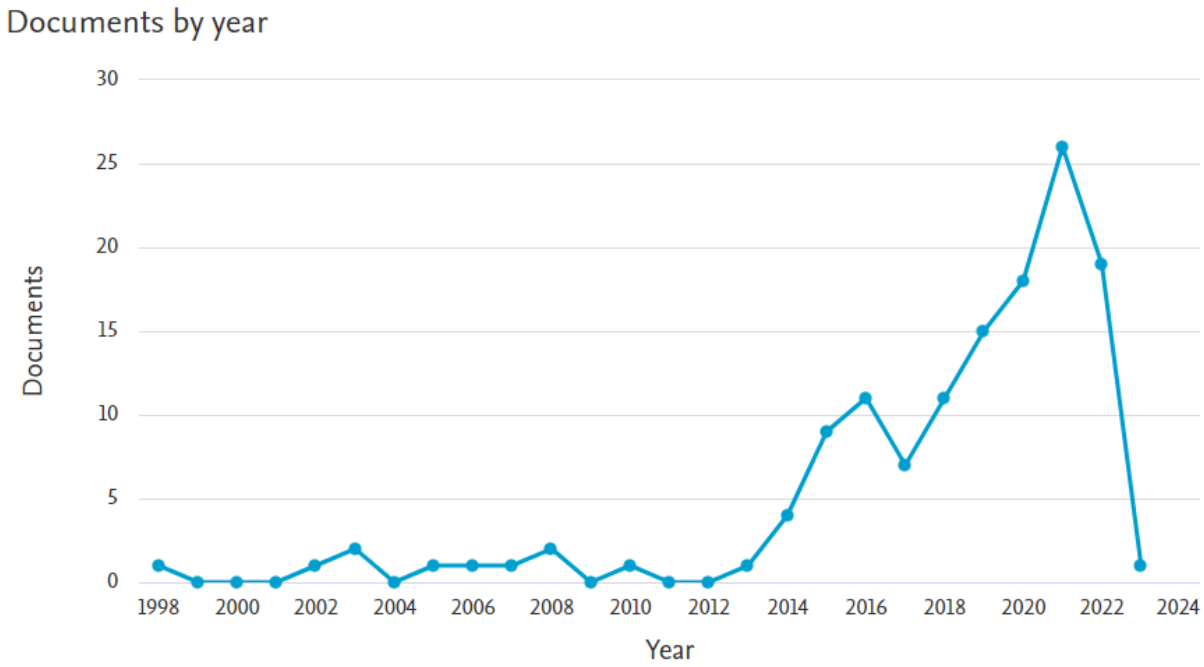


Рисунок 2. Динаміка публікацій, присвячених дослідженню кіберзагроз фінансових систем.

За аналітикою системи SciVal бази даних Скопус за період 2019-2022 рр. безпека кіберпростору стосуються великої кількості галузей, найбільший за обсягом кластер, сформований «сніжними кульками» сірого кольору, що стосується галузі комп'ютерних наук. Загальна кількість тем у сформованих 537 кластерах складає 2 905 одиниць.

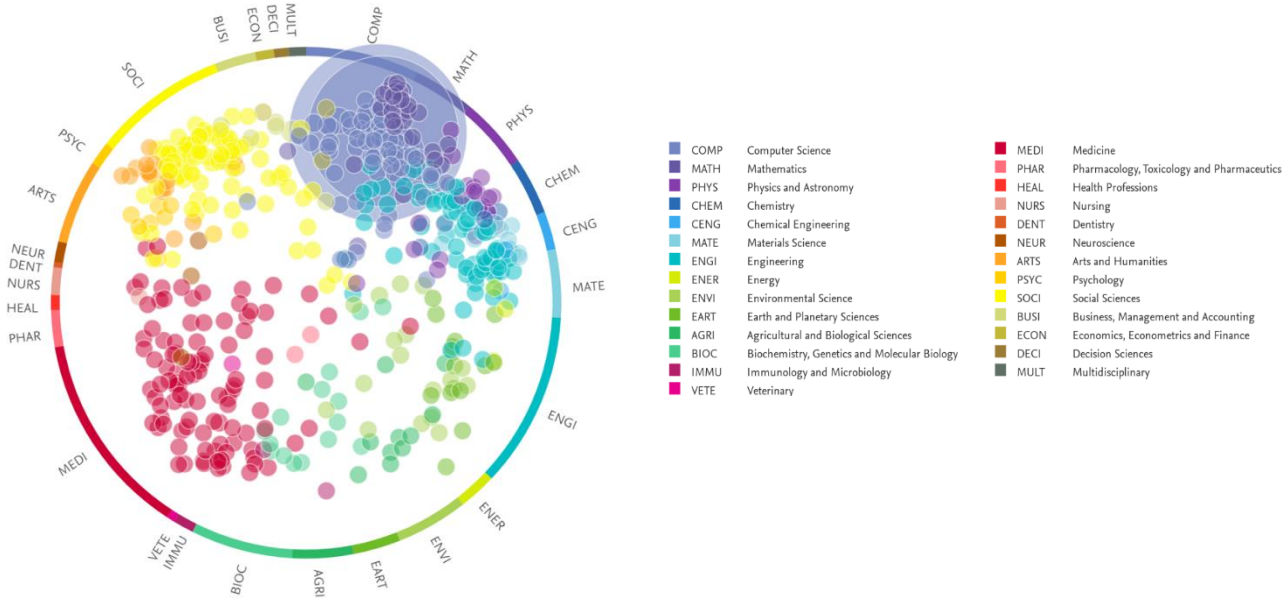


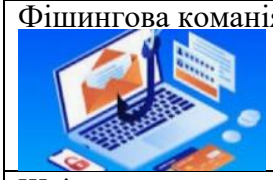
Рис. 3. Предметні галузі наукових публікацій за тематикою «безпека кіберпростору» (Cyberspace security)

2. Сучасні типи кіберзагроз фінансової системи України та Європи

В Україні у 2017 році створено Центр кіберзахисту Національного банку України, який поєднує та координує зусилля у сфері забезпечення кібербезпеки та кіберзахисту в банківському та фінансовому секторах України. З 2018 року у складі Центру кіберзахисту Національного банку України [3] функціонує команда реагування на кіберінциденти в банківській системі (CSIRT-NBU). У серпні 2019 року Центр кіберзахисту Національного банку України та Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України підписали Меморандум про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту, спрямовану на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та кіберзахисту. За цих умов необхідність комплексного та всебічного аналізу ризику фінансових шахрайств, особливо кібершахрайств, їх прогнозування та упередження, блискавичне реагування на щонайменші прояви злочинності та кіберзлочинності як з боку фінансової установи, так і на рівні держави є постійно актуальною задачею сьогодення та прийдешнього п'ятиліття.

За даними Центр кіберзахисту Національного банку України основними типами кіберзагроз у 2022-2023 роках, є кіберзагрози, що наведені в таблиці 2.

Таблиця 2 – Кіберзагрози у фінансовій системі України

Кіберзагроза	Опис
Зафіксована фішингова кампанія EMOTEN 	Вкладені .doc файли містять макроси. Для маскування вихідного коду макросів використано технологію VBA stomp, що дозволяє обходити деякі системи антивірусного захисту.
Фішингова комапія 	Метою розсилання листів є отримання авторизаційних даних користувача (пароль, електронна адреса). Листи містять посилання для проходження процедури верифікації електронної пошти на фейковій сторінці.
Шкідливе програмне забезпечення #MassLogger 	Розсилання шкідливих електронних листів з вкладення типу .xlsx за допомогою якої відбувається експлуатація вразливості CVE-2017-11882 для завантаження шкідливого посилання.
Зловмисне програмне забезпечення #GuLoader 	Розсилання шкідливих електронних листів, що містять у тілі листа стилізоване під ярлик документу pdf зображення з активним посиланням на завантаження із хмарного сховища архіву із шкідливим програмним забезпеченням GuLoader. Під час відпрацювання експлуатується техніка thread injection та завантажується зашифрований модуль із функціоналом NetWire RAT.

Кіберзагроза	Опис
Розсилання шкідливих електронних листів #COVID19 	Зафіксовано розсилання електронних листів, що замасковані під щоденний звіт COVID-19 та рекомендовані міри захисту від пандемії. Отримані листи містять шкідливі вкладення типу rtf та доставляють до користувачів шкідливе програмне забезпечення #AveMaria, в обхід вбудованого механізму захисту ОС Windows - AMSI.
Розсилання шкідливих електронних листів CVE-2017-11882 	Розсилання шкідливих електронних листів, що містять вкладення типу .xlsx, у вкладенні листів знаходяться документи Request for Quotation.xlsx, Product Specication.xlsx, що містить ole-об’єкти.
Зловмисне програмне забезпечення Netwire RAT 	Розсилання зловмисного програмного забезпечення, яке використовується для дистанційного керування зараженим ПК. Може здійснити більше 100 шкідливих дій на заражених ПК, записувати інформацію введену з клавіатури та поведінку миші, робити знімки екрана, перевіряти інформацію про систему та створювати підроблені проксі-сервери.

Джерело: побудовано на основі даних порталу Центру кіберзахисту Національного банку [3]

Перелік сучасних кіберзагроз у фінансовій системі Європи (за даними Агентства Європейського Союзу з кібербезпеки) такий:

1. Фішинг. Фішинг є найпоширенішою кіберзагрозою для європейської фінансової системи [4]. Це передбачає надсилання електронних листів або текстових повідомлень, які нібито надходять із законних джерел, щоб обманом змусити людей розкрити конфіденційну інформацію, таку як паролі чи реквізити банківського рахунку.

2. Шкідливе програмне забезпечення – це програмне забезпечення, призначене для проникнення в комп’ютерну систему, викрадення даних і порушення роботи. Зловмисне програмне забезпечення можна встановити на комп’ютери через шкідливі веб-сайти, посилання або завантаження. Кіберзлочинці можуть використовувати зловмисне програмне забезпечення для доступу та маніпулювання фінансовими даними або крадіжки грошей з банківських рахунків.

3. Соціальна інженерія: соціальна інженерія – це тип атаки, яка використовує психологічні маніпуляції, щоб обманом змусити людей розкрити конфіденційну інформацію або виконати певні дії. Кіберзлочинці можуть використовувати соціальну інженерію, щоб отримати доступ до фінансових рахунків або викрасти гроші.

4. Порушення даних: Порушення даних відбувається, коли кіберзлочинці отримують доступ до конфіденційних даних організації, таких як фінансові записи або інформація про клієнтів. Порушення даних може призвести до значних фінансових втрат, а також до репутації.

5. Програми-вимагачі. Програми-вимагачі – це різновид шкідливих програм, які блокують комп'ютер або дані користувача, доки не буде сплачено викуп. Кіберзлочинці можуть використовувати програми-вимагачі, щоб вимагати оплату в обмін на доступ до фінансової інформації або рахунків.

На рисунку 3 відображено прогнозовані типи кіберзагроз на 2030 рік.

Рисунок 3. Прогноз кіберезагроз за даними Агентства Європейського Союзу з кібербезпеки (ENISA)

Компанії, банки, фінансові установи, підприємства (всі соціально-економічні об'єкти) повинні стежити за станом кібербезпеки та мати надійний захист від потенційних атак, а також повинні застосовувати безпечні методи автентифікації клієнтів і шифрування даних, щоб захистити конфіденційні дані клієнтів. Зокрема, Агентство Європейського Союзу з кібербезпеки (ENISA) рекомендує дотримуватися 12 кроків для якісної кібербезпеки ведення бізнесу малими та середніми підприємствами (табл. 4) [5].

Таблиця 4. Заходи кібербезпеки малих та середніх підприємств (МСП)

Назва заходу	Короткий опис заходу
1. Розвивати гарну культуру кібербезпеки: призначити відповідальну особу за організацію кібербезпеки; проводити аудити кібербезпеки; пам'ятати про захист даних	1.1. Надійна кібербезпека – запорука сталого розвитку та успіху будь-якого бізнесу. Тому необхідно призначити відповідальну особу, яка повинна забезпечити відповідні ресурси, такі як час від персоналу, придбання програмного забезпечення, послуги і обладнання для кібербезпеки, навчання персоналу та розвиток ефективної політики щодо кібербезпеки. Крім того необхідно мати відкриту підтримку керівництва щодо ініціатив у сфері кібербезпеки, проведення відповідних тренінгів для співробітників та надання чітких, конкретних правил, викладених у політиках кібербезпеки, що регулярно переглядаються та оновлюються. 1.2. У політиках мають бути

	прописані наслідки, з якими може зіткнутися працівник, якщо не буде дотримуватимуться політики кібербезпеки. Регулярні аудити повинні проводитися особами, які мають відповідні знання, навички та досвід та не залежать від щоденних ІТ-операцій. 1.3 Згідно із Загальним регламентом ЄС щодо захисту даних, будь-які підприємства, фінансові установи, які обробляють або зберігають персональні дані резидентів Європейської економічної зони, повинні забезпечити відповідні засоби контролю безпеки для захисту цих даних. Це гарантує захист інтересів третіх сторін, які працюють від імені відвідного підприємства, та надає їм заходи безпеки [6].
2. Забезпечити відповідне навчання	Проводити регулярні тренінги з кібербезпеки для всіх співробітників, щоб вони могли розпізнавати різні загрози кібербезпеці та боротися з ними. Ці тренінги мають бути адаптовані для малих підприємств та зосереджені на реальних ситуаціях
3. Забезпечити ефективне управління третьою стороною	Переконатися, що всі постачальники, особливо ті, хто мають доступ до конфіденційних даних та/або систем, активно керуються та відповідають узгодженим рівням безпеки. В контрактних угодах повинно бути прописано, як постачальники відповідають вимогам безпеки
4. Розробити план реагування на інциденти	Офіційний план реагування на інциденти має містити чіткі вказівки, ролі та обов'язки, задокументовані для забезпечення своєчасного, професійного та належного реагування на всі інциденти безпеки. Для того, щоб швидко реагувати на загрози безпеці, необхідно досліджувати та аналізувати інструменти, що можуть відстежувати та створювати сповіщення, за умов підозрілих дій або порушення безпеки.
5. Безпечний доступ до систем	Використовувати фразу-пароль, що є набором принаймні трьох випадкових поширених слів, об'єднаних у фразу, яка забезпечує дуже хороше поєднання запам'ятовуваності та безпеки: не використовувати повторно в іншому місці; не діліться з колегами; увімкнути багатофакторну автентифікацію; використовувати спеціальний менеджер паролів. За умов використання типового паролю, рекомендовано робити його довгим, із символами верхнього та нижнього регістру та спеціальними символами. Уникати використання «123», «пароль», особистої інформації, що є відкритому доступі в Інтернеті.
6. Безпека пристороїв	Ключовим кроком у програмі кібербезпеки є забезпечення безпеки пристроїв, якими користуються співробітники (настільні ПК, ноутбуки, планшети чи смартфони), тому необхідно зберігати програмне забезпечення виправленим та оновленим (в ідеалі використовувати централізовану платформу для керування виправленнями). 6.1. Централізоване кероване антивірусне ПЗ має бути впроваджено на всіх типах пристроїв та підтримуватися в актуальному стані, щоб забезпечити його постійну ефективність. 6.2. Використовувати ПЗ для блокування електронних листів зі спамом, електронних листів із посиланнями на шкідливі веб-сайти, електронних листів із шкідливими вкладеннями, вірусами, фішингових електронних листів. 6.3. Захист даниз через шифрування. Малі та середні

	підприємства повинні гарантувати, що дані, що зберігаються на мобільних пристроях, таких як ноутбуки, смартфони зашифровані. Для даних, що передаються через загальнодоступні мережі, такі як мережі Wi-Fi готелів чи аеропортів, переконайтеся, що дані зашифровані, використовуючи віртуальну приватну мережу (VPN) або доступ до веб-сайтів через безпечне з'єднання за допомогою протоколу SSL/TLS. Переконайтеся, що на їхніх власних веб-сайтах використовується відповідна технологія шифрування для захисту даних клієнтів під час їх передачі через Інтернет.
7. Безпека мережі	Спрощуючи роботу персоналу віддалено, багато МСП дозволяють персоналу використовувати власні ноутбуки, планшети та/або смартфони. Це викликає кілька проблем із безпекою конфіденційних бізнес-даних, що зберігаються на цих пристроях. Одним із способів управління цим ризиком є керування мобільними пристроями. Це дозволить: здійснювати контроль над пристроями, яким дозволено користуватись послугами й системами МСП; на таким пристроях має бути встановлене актуальне сучасне антивірусне ПЗ; доступ до таких пристроїв – через надійні паролі або PIN-код; дистанційно стерти будь-які дані МСП з пристрою, якщо власник пристрою повідомить про втрату чи викрадення пристрою, або якщо робота власника пристрою закінчиться з МСП. Наступна рекомендація – використовувати брандмауери та регулярно перевіряти роботу та налаштування пристроїв, що залучені у віддаленому доступі до ресурсів МСП.
8. Удосконалення фізичної безпеки	Усюди, де міститься важлива інформація, слід застосовувати відповідні засоби фізичного контролю. Наприклад, службовий ноутбук або смартфон не можна залишати без нагляду на задньому сидінні автомобіля. Кожен раз, коли користувач відходить від свого комп'ютера, він повинен заблокувати його. В іншому випадку потрібно увімкнути функцію автоматичного блокування на будь-якому пристрої, який використовується для комерційних цілей. Конфіденційні друковані документи також не слід залишати без нагляду, а якщо вони не використовуються, надійно зберігати.
9. Захист резервних копій	Резервне копіювання має бути регулярним та автоматизованим, бажано шифрувати резервні копії. Проводити тестування щодо здатності відновлення. В ідеалі слід проводити регулярне тестування повного відновлення від початку до кінця.
10. Синхронізувати з хмарними технологіями	Пропонуючи багато переваг, хмарні рішення все ж представляють деякі унікальні ризики, які МСП слід враховувати перед тим, як співпрацювати з постачальником хмарних технологій. ENISA опублікувала «Посібник з хмарної безпеки для малих і середніх підприємств» [7], до якого малим і середнім підприємствам слід звернутися під час переходу на хмару. Вибираючи хмарного постачальника, МСП має переконатися, що він не порушує жодних законів чи правил, зберігаючи дані, особливо персональні, за межами ЄС/ЄЕЗ. Наприклад, Загальний регламент захисту даних (GDPR) ЄС вимагає, щоб персональні дані жителів ЄС/ЄЕЗ не зберігалися та не

	передавалися за межі ЄС/ЄЕЗ, за винятком дуже особливих умов.
11. Захист онлайн-сайтів	Вкрай важливо, щоб МСП гарантували, що їхні онлайн-сайти налаштовані та обслуговуються безпечним способом і що будь-які персональні дані або фінансові деталі, такі як дані кредитної картки, належним чином захищені. Це передбачає проведення регулярних тестів безпеки веб-сайтів для виявлення будь-яких потенційних слабких місць у безпеці та проведення регулярних перевірок для забезпечення належного обслуговування та оновлення сайту.
12. Шукати та ділитись інформацією	Ефективним інструментом боротьби з кіберзлочинністю є обмін інформацією. Обмін інформацією щодо кіберзлочинності є ключовим для того, щоб МСП краще розуміли ризики, з якими вони стикаються. Компанії, які дізнаються про виклики кібербезпеки та про те, як ці проблеми вдалося подолати, з більшою ймовірністю вживуть заходів для захисту своїх систем, ніж якби вони почули подібні подробиці з галузевих звітів або опитувань щодо кібербезпеки.

Джерело: побудовано на основі [5].

3. Аналіз факторів цифрової довіри

Відповідно до аналітичного звіту «Економічна правда» довіра українців до фінансових установ у 2018 році знаходилася на рівні близько 20% [8]. Повністю довіряють фінансовим установам лише 3%. Для порівняння, аналогічний показник, наприклад, у Чехії становить 80%.

Факторів довіри багато, але серед ключових – ефективна система гарантування вкладів. І вона потребує еволюційних змін.

Проте сама по собі система гарантій не дасть швидкого результату. Для відновлення репутації фінансового сектору та довіри населення потрібна злагоджена робота всіх учасників фінансового сектору та державних інституцій. В умовах конвергенції процесів цифровізації в фінансово-економічинх системах доцільним розглянути зміст факторів цифрової довіри та ступінь взаємозв'язку між ними.

Інформаційно-статистичною базою використано дослідження науковців всесвітньо відомої школи Флетчера щодо індексу цифрової еволюції. Наукова школа функціонує при університеті Тафтса та активно займається дослідженнями міжнародних відносин та ведення бізнесу [9]. Отже для дослідження використаємо систему показників цифрової довіри, що охоплює групу з 42 економік, серед переліку яких країн-членів ЄС – 13 (Австрія, Белгія, Данія, Німеччина, Іспанія, Франція, Ірландія, Італія, Нідерланди, Польща, Португалія, Румунія, Швеція). Система містить чотири ключових драйвери-фактори: ставлення та поведінка, цифрове середовище, цифровий досвід користувача. Саме ці фактори враховують надійність цифрової екосистеми, рівень і типи суперечностей (тертя) в цифровому досвіді, рівень довіри громадян

до цифрової екосистеми та глибину залучення користувачів Інтернету. Так категорія ставлення до цифрової довіри визначається двома індикаторами, що формуються на основі опитування населення досліджуваних країн щодо їх інтуїтивного ставлення до соціальних процесів цифровізації (К1) та довіри до науки та цифрових технологій (К2). Категорія поведінки в цифровому просторі визначається показником попиту на соціальні мережі (К3), толерантністю до тертя (К4) (визначають проблеми з доступом, ідентифікацією, інфраструктурою при здійсненні фінансової транзакції), складність цифрового платежу (К5), використання електронної комерції та мобільних платежів (К6), використання соціальних мереж (К7), використання технологій (К8). Фактор довіри до цифрового середовища визначається за допомогою індикаторів конфіденційності (К9), безпеки К10) та звітності гарантів – надавачів цифрових послуг (К11). Четвертий фактор – фактор цифрового досвіду користувача визначається показниками, що характеризують проблем доступу (К12), проблем інфраструктури (К13) та проблему взаємодії (К14).

Практична реалізація щодо формування пар канонічних кореляцій здійснена за допомогою програмного забезпечення Statgraphics 19 з використанням процедури Multivariate/Canonical Correlations. Перевірка значущості кореляційного зв'язку здійснюється шляхом використання стандартного статистичного критерію α (P-Value – рівень значущості не повинен перевищувати 5%), статистики Лямбда Уилкса (характеризує якість дискримінантного аналізу щодо однорідності груп, чим ближче значення до 0, тим кращий буде розподіл) та критерію Хі-Квадрат. Результати аналізу дозволили визначити 5 пар канонічних кореляцій (формули (1) – (5)) між цифровим середовищем та ставленням до цифрової довіри (табл. 5), між поведінкою в цифровому просторі та цифровим середовищем (табл. 6), між поведінкою в цифровому просторі та цифровим досвідом користувачів (табл. 7), між цифровим середовищем та цифровим досвідом користувачів (табл. 8).

Таблиця 5

Статистичні характеристики канонічних кореляцій між категоріями «цифрове середовище» та «ставлення користувачів до цифрової довіри»

№	Власні числа	Коеф. канонічних кореляцій	Статистика Лямбда Уилкса	Статистика Хі-Квадрат	Число ступенів свободи	Рівень значущості
1	0,370751	0,608893	0,615988	18,4121	6	0,0053
2	0,021074	0,145169	0,978926	0,809371	2	0,6672

Джерело: обчислено у пакеті Statgraphics 19

В таблиці 5 статистично значимий взаємозв'язок першої пари (P-Value ≤ 5%), коефіцієнт кореляції між ними $r_{U_1V_1}$ = 0,608893 та характеризує високу силу взаємозв'язку. Модель канонічних кореляцій між складовою соціального та поведінкового спрямовування така:

$$\begin{cases} U_1 = -0{,}892K_9 + 0{,}345K_{10} + 0{,}183K_{11}, \\ V_1 = 0{,}008K_1 + 0{,}999K_2. \end{cases} \quad (1)$$

Внесок кожного індикатора у значення канонічної змінної визначається за абсолютною величиною коефіцієнта: чим більше значення, тим більший внесок (Canonical Correspondence Analysis).

Таблиця 6

Статистичні характеристики канонічних кореляцій між категоріями «поведінка в цифровому просторі» та «цифрове середовище»

№	Власні числа	Коеф. канонічних кореляцій	Статистика Лямбда Уилкса	Статистика Хі-Квадрат	Число ступенів свободи	Рівень значущості
1	0,573649	0,757396	0,270593	47,057	18	0,0002
2	0,266743	0,516471	0,634671	16,3673	10	0,0896
3	0,134449	0,366673	0,865551	5,19802	4	0,2676

Джерело: обчислено у пакеті Statgraphics 19

Таблиця 6 відображає три пари взаємозв'язків, проте статистично значимий взаємозв'язок першої пари, коефіцієнт кореляції між ними $r_{U_1V_1}$ = 0,757396. Модель канонічних кореляцій між факторами поведінки в цифровому просторі та цифровим середовищем подано формулою (2):

$$\begin{cases} U_1 = -0{,}166K_3 - 0{,}487K_4 + 0{,}073K_5 + 0{,}348K_5 - 0{,}603K_7 - 0{,}337K_8, \\ V_1 = 0{,}148K_9 + 0{,}546K_{10} + 0{,}435K_{11}. \end{cases} \quad (2)$$

Таблиця 7

Статистичні характеристики канонічних кореляцій між категоріями «поведінка в цифровому просторі» та «цифровий досвід користувачів»

№	Власні числа	Коеф. канонічних кореляцій	Статистика Лямбда Уилкса	Статистика Хі-Квадрат	Число ступенів свободи	Рівень значущості
1	0,519138	0,720512	0,281862	45,5881	18	0,0003
2	0,40577	0,637001	0,586161	19,2298	10	0,0374
3	0,0135796	0,116531	0,98642	0,492214	4	0,9743

Джерело: обчислено у пакеті Statgraphics 19

Канонічні кореляції між категоріями, що визначають поведінку в цифровому просторі та досвід користувачів (табл. 7) є статистично значущими для двох пар (3, 4), значення коефіцієнтів кореляцій складають $r_{U_1V_1}$ = 0,720512 та $r_{U_2V_2}$ = 0,637001 відповідно:

$$\begin{cases} U_1 = -0{,}107K_3 + 0{,}231K_4 + 0{,}838K_5 + 0{,}210K_5 - 0{,}179K_7 + 0{,}169K_8, \\ V_1 = -0{,}243K_{12} - 0{,}070K_{13} + 1{,}212K_{14}. \end{cases} \quad (3)$$

$$\begin{cases} U_2 = 0{,}115K_3 - 0{,}244K_4 - 0{,}102K_5 + 0{,}240K_5 - 0{,}723K_7 - 0{,}527K_8, \\ V_2 = 1{,}136K_{12} + 0{,}765K_{13} - 1{,}131K_{14}. \end{cases} \quad (4)$$

Таблиця 8

Статистичні характеристики канонічних кореляцій між категоріями між цифровим середовищем та цифровим досвідом користувачів

№	Власні числа	Коеф. канонічних кореляцій	Статистика Лямбда Уилкса	Статистика Хі-Квадрат	Число ступенів свободи	Рівень значущості
1	0,671579	0,819499	0,279393	47,8176	9	0,0000
2	0,149056	0,386077	0,850715	6,06293	4	0,1945
3	0,000269459	0,0164152	0,999731	0,0101061	1	0,9199

Джерело: обчислено у пакеті Statgraphics 19

Статистично значущий взаємозв'язок між складовими цифрового середовища та досвідом користувачів (табл. 8) з коефіцієнтом кореляції $r_{U_1V_1}$ = 0,819 подано моделлю (5):

$$\begin{cases} U_1 = 0{,}202K_9 + 0{,}348K_{10} + 0{,}580K_{11}, \\ V_1 = 1{,}060K_{12} + 0{,}683K_{13} - 0{,}757K_{14}. \end{cases} \quad (5)$$

Отже, отримані моделі (1-5) підтверджують якість ознакового простору щодо визначення та опису цифрової довіри, а індикатори, що визначають ключові фактори (ставлення до цифрової довіри, поведінка в цифровому середовищі, цифрове середовище, цифровий досвід користувача) можуть бути використані для подальшого розроблення економетричних моделей залежності рівня цифрової довіри, виявлення потенційних та латентних ознак щодо підвищення рівня цифрового розвитку країни, посилення безпеки здійснення всіх нагально-необхідних операцій в умовах сьогодення, особливо фінансово-економічного спрямування, формування безпечного цифрового середовища як запоруки цифрової конкурентоспроможності.

Залежність від цифрових систем фінансово-економічних, політичних, соціальних сфер, трансформація майже всіх процесів життєдіяльності громадян, бізнесів, медицини в напрямку переходу від фізичного реального до цифрового віртуально-дистанційного під впливом глобальної пандемії, з одного боку, та інтелектуалізації суспільства – з іншого, зумовлюють необхідність комплексного аналізу рушійних категорій індикаторів цифрової еволюції, цифрової довіри та стійкості цифрової інфраструктури до викликів сьогодення. В розрізі кожної країни актуальним та надзвичайно важливим завданням є формування стійкого, надійного цифрового середовища, як визначальної детермінанти цифрової конкурентоспроможності та посилення фінансової безпеки.

Фінансовий сектор особливо вразливий до кіберзагроз через широке використання Інтернету, мобільних банківських технологій та інших інноваційних технологій, які постійно розвиваються. Крім того, фінансові компанії також повинні керувати доступом до конфіденційних даних, а також гарантувати, що сервіси третіх сторін відповідають нормативним вимогам.

Соціально-економічні об’єкти (фінансові установи, команії, банки, фірми, МСП) повинні бути в курсі останніх векторів загроз і розробити надійні засоби захисту від них, такі як брандмауери, системи виявлення вторгнень і програми захисту від шкідливих програм. А також повинні проводити аналіз теплової карти, щоб виявити потенційні зони вразливості. Нарешті, необхідно проводити тренінги з питань безпеки для працівників на постійній основі, щоб гарантувати, що працівники добре поінформовані про своє середовище та найкращі практики безпеки.

Список використаних джерел

1. Strategic plan 2020-2024 – Informatics. URL : https://ec.europa.eu/info/publications/strategic-plans-2020-2024-informatics_en
2. Правління Національного банку України Постанова 12.08.2022 № 178: Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
3. CSIRT-NBU. URL: https://cyber.bank.gov.ua/last-ios-news
4. Phishing most common Cyber Incident faced by SMEs. URL: https://www.enisa.europa.eu/news/enisa-news/phishing-most-common-cyber-incidents-faced-by-smes
5. Cybersecurity guide for SMEs - 12 steps to securing your business. URL: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
6. Data protection Rules for the protection of personal data inside and outside the EU. URL: https://commission.europa.eu/law/law-topic/data-protection_en
7. Cloud Security Guide for SMEs. URL: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes
8. Рецепти довіри до фінансових установ: Економічна правда. URL: https://www.epravda.com.ua/columns/2018/11/6/642331/
9. Bhaskar Chakravorti, Ravi Shankar Chaturvedi, Christina Filipovic, and Griffin Brewer (2020). Digital in the Time of COVID. Trust in the Digital Economy and Its Evolution Across 90 Economies as the Planet Paused for a Pandemic. Tufts University, The Fletcher School, 2020. 80 P.